



Owner-Operator's Business  
Association of Canada

Association professionnelle des  
routiers autonomes du Canada

*...from the  
director's chair*

## Big Brother Is *Already* Watching

Few things symbolize the post-9/11 Western world more than the iconic surveillance camera. When strange-looking vans began prowling the streets of Canadian cities earlier this year snapping pics for Google's controversial Street View feature, the ire of privacy watchdogs across the country was raised. And when electronics systems provider Sierra Nevada Corporation, hoping to grab the attention of US Homeland Security, hoisted a high-tech camera in a balloon over Port Huron/Sarnia to monitor the St. Clair River and the Blue Water Bridge, normally polite Canadians were motivated to stage a cheeky "Moon the Balloon" protest.

Many other forms of surveillance aren't quite so obvious, and don't inspire the sort of mistrust associated with eyes in the sky, yet they're often far more effective at capturing personal information that can affect our lives dramatically.

At the same time many truckers are concerned about electronic monitoring of their activities with black boxes, electronic logs, and even cab cams, they're freely giving away information that's far more personal and probably no less sensitive.

We're spending increasing amounts of time hanging with our friends on various social networks – Facebook, MySpace, Twitter, and others – and increasingly, marketers, employers, and law enforcement officials watch those sites to find out what we're up to.

Discussions about our whereabouts and activities, likes and dislikes, hobbies, vacation plans, and even those "25 random things" lists we share with our Facebook pals provide valuable insight into our personal and professional lives, and leave behind indelible records that can come back to haunt us.

Records such as the time you posted a message, for example. While there are lots of time markers DOT might use to verify your logs, in cases involving fatalities, officials have used

Facebook and MySpace postings. Some of my trucker friends give detailed information on Facebook about where they are and when they're picking up and delivering, and it wouldn't be difficult to build a case against them if their logs failed to match their Facebook trail.

Is the prospect of law enforcement monitoring our Internet presence something that drivers should be concerned about, or are we just being paranoid? A few weeks ago, Canada's privacy commissioner released a report about Facebook's privacy policies – or maybe I should say the lack thereof.

The commissioner concluded that some of Facebook's policies violated Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which specifies how private sector organizations may collect, use, or disclose personal information in the course of commercial activities. For example, Facebook shares its users' personal information with some 950,000 third-party games, quiz, and entertainment developers from around the world – without the user's "meaningful" consent.

The investigation also found that Facebook keeps information from accounts deactivated by users indefinitely. Users can "deactivate" an account, but not delete it, and data such as photographs remain on Facebook servers long after an account is supposedly closed.

More troubling was the practice of providing personal information about non-users – without their consent. For example, users can tag photos and videos of non-users with their names, and provide e-mail addresses so Facebook can invite them to join the site. Ever get one of those messages from Facebook? Ever wondered how they got your e-mail address?

That kind of information in and of itself might seem innocent enough, but when it's cross-referenced and put together it can be quite revealing. We know marketers just gobble up that kind of



**Joanne  
Ritchie:  
OBAC  
executive  
director**

information, and it's used increasingly by employers as an electronic background check – sort of an electronic CV. Have you ever posted anything on a social networking site you wouldn't want your boss to read?

A recent study called *Social Networking: 2009* conducted by Ipsos Reid, a leading public opinion research firm, revealed that the majority of Canadians now have an online social network profile (over 85% of them use Facebook), and many now spend more than one-third of their Internet time each week participating in and browsing online social network sites. There's little doubt that Facebook and the others are here to stay, and they can be a great deal of fun, but we need to be careful as we post, poke, and tweet our way through cyberspace.

But, before you accuse me of being paranoid, I want to stress that the issue here is not that Big Brother – and lots of others – are watching, it's that we should be mindful of the footprint we leave after we log off. We need to find a balance between using these new communications and networking tools and revealing a bit too much about ourselves. We can't take privacy issues lightly anymore.

Some interesting discussion is still to come on this subject as the day of EOBRs, cab cams, and other electronic surveillance looms closer. You have a choice when it comes to online social networking, but DOT-mandated video cameras in your cab are another matter altogether. We can't afford to let someone else write all the rules next time.